# Framework for Trust with eIDAS compliance, EBSI compliance and Qualified Service Providers

Erwin Nieuwlaar
*Delft University of Technology*
March 2022

## Contents

**1 Introduction** **1**

**2 Problem Description** **2**

**3 Background** **3**

**4 Design** **3**

**5 eIDAS** **3**

**6 Infrastructure** **3**
6.1 TrustChain . . . . . . . . . . . . . . . . . . 3
6.2 IPv8 . . . . . . . . . . . . . . . . . . . . . . 3
6.3 EBSI compliance . . . . . . . . . . . . . . 3

**7 Qualified Trust Service Providers** **3**
7.1 Legally binded trust . . . . . . . . . . . . 3
7.2 KVK Handelsregister . . . . . . . . . . . . 3
7.3 RDW Vehicle Register . . . . . . . . . . . 3
7.4 Basisregistratie Personen . . . . . . . . . . 3

**8 Implementation** **3**

**9 Conclusion** **3**
9.1 Future Work . . . . . . . . . . . . . . . . 3

## 1 Introduction

Citizens must be able to comprehend their digital world, select how they want to interact with it, and act autonomously. At the moment, this is not obvious in the digital realm. Although technology is getting simpler to use, it is becoming more difficult to comprehend precisely how it operates and how data, whether personal or not, is used. This may be enhanced by, among other measures, reducing data acquisition. In order to reduce the current data economy, the European Union, and accordingly, the Dutch government is striving to develop an alternative to the current data economy, which relies too much on vast data collecting and processing [1]. With the Data Governance Act [2] and the Data Act [3], the European Commission is pushing a data economy in which user-friendly systems are the standard for controlling data. And wherever firms and governments have legal access to the data they need without obtaining it from parties that do not respect European principles. With the European Data Act, the European Union is developing standards for fair access to and use of non-personal data, including the right to access data and the ability to readily transfer data to other parties. The new Data Act addresses genuine rights to access and use data. A new, more privacy-friendly method of processing data, in which people are given actual options, does not spontaneously appear. European citizens will obtain a digital identity that is widely useable so that they may securely identify themselves in the digital world and have more control over their own data - similar to using a passport in the physical world [4]. These means of identification enable us to establish our identity. By using digital identification, we can streamline interactions and save time. Digital identity tools are presently available from a variety of private and public suppliers, for instance enabling consumers to utilize online banking or various public services. There are several levels of security and reliability offered by digital IDs, the most universal European standard (and solely used in this paper) is the Level of Assurance provided in the eIDAS regulation [5]. At the moment, large platforms allow their users to login to a variety of online services, like shopping and reading the news, but these logins do not provide consumers complete choice over the information they submit to identify themselves with online services. These means of identification provided by Big Tech control most of the market share [6] and induce privacy issues [7]. Although the European Commission has not set a strict release date for the new European digital identity, the first toolbox to experiment with implementation should be released by 30 October 2022 [8]. The most innovative aspect of the new regulation with regard to the new European digital passport is that everyone will be entitled to a European Digital Identity Wallet that is recognized by all Member States. However, there will not be any obligation either. The European Digital Identity Wallet will be designed as a Self-Sovereign Identity Wallet where users choose to disclose their personal information with online services, enabling people to digitally identify themselves, as well as store and manage identity data and official documents in an electronic format. These may include a driver's license, a prescription, or educational certification. With the wallet, users will be able to access internet services, transfer digital documents, or simply confirm a certain personal trait, such as age, without disclosing their identity or other personal information. While the European Digital Identity will be required to be recognized by public services and some commercial services, its security characteristics entice all private service providers to recognize it for services that demand rigorous authentication, opening up new economic prospects which could lead to a 3 to 13% increase of GDP by 2030 if integrated successfully [9]. Three of such potential economic prospects is the integration of the Company Register from the Netherlands Chamber of Commerce, the Vehicle Registry of the Netherlands Vehicle Authority, and the Netherlands Personal Records Database. These institutions will be Qualified Trust Service Providers, and will serve as an anchor for legal certainty for Dutch persons and businesses. In this work, we will provide alignment of notions within Self-Sovereign Identity, eIDAS, and EBSI, provide a framework for eIDAS and EBSI integration in a Self-Sovereign Identity environment such as the coming European Digital Identity Wallet, and implement a use case in collaboration with the Netherlands Chamber of Commerce, Netherlands Vehicle Authority and the Personal Records Database.

# 2 Problem Description

In utopia an user would have full control, independence and access over all their data where their rights are protected, sharing of data is done minimally and with consent. Nonetheless, the system should be transparent, interoperable, portable and persistent [10]. This vision with regard to identity is often seen as the preeminent Self-Sovereign Identity (not all opinions are aligned on this matter [11, 12]), where people or organizations have exclusive ownership of their digital and analog identities, as well as control over the sharing and use of their personal data. Aforementioned, the European Commission envisions a similar perception with the upcoming European Digital Identity wallet [13]. However, the steps that should be taken from the current means of identification and authentication to a fully operational Self-Sovereign Identity, such as the European Digital Identity, have a steep slope. Below is a list of the current challenges in the field of Self-Sovereign Identity and the application thereof [14].

1. Protocols, practices, and rules pertaining to data management, data interchange, and user experience should be created and executed with care. The system should be user-centric, compliant to regulations, and consistent with the Privacy by Design and Security by Design principles.

2. In the Self-Sovereign Identity paradigm, the users are responsible for key-management and the accompanying risks. Numerous examples exist in which users have lost their cryptographic keys, resulting in the loss of vital data [15] or irretrievable capital [16]. Resolving the core management needs of the Self Sovereign Identity architecture is a prerequisite for the widespread adoption of Self Sovereign Identity. Where dependence on decentralized key custodians is one solution to the difficulty of key management [17].

3. The user's consent must be significant, unambiguous, explicit, well-formed, freely granted, and describe clear choices. This procedure is difficult to implement and validate using existing identification models. In addition, requiring users to accept to several privacy rules and data sharing practices has resulted in a phenomenon known as *consent fatigue* [18], in which the user is inundated with privacy alerts. Furthermore, consent management, presentation, and enforcement should be considered.

4. Distributed ledger technology is the foundation of many Self-Sovereign Identity systems. Certain distributed ledgers are public, enabling any entity to access or write to the ledger, whilst others are permissioned and only let a limited number of allowed entities to read or write new data into the ledger. The permissioned method runs the danger of developing a centralized and censored architecture comparable to an oligopoly among the few permitted entities if it is not properly constructed [19, 20]. The permissionless and public paradigm, on the other hand, are susceptible to assaults prevalent in open distributed ledger systems [21].

5. It is essential to recognize and communicate the necessary level of decentralization required to meet the preceding mentioned Self-Sovereign Identity vision. Certain identity management processes, such as identity claim issuance, identity search, and safe data storage, may rely on centralization and trusted intermediates to varying degrees. Some implementations of Self-Sovereign Identity give considerable power in the hands of a small number of trusted entities that must adhere to a shared contractually binding trust structure, possibly making these entities the network's weakest link. An example is of a governance system using machine-readable showing several problems in the past [20]. Efforts to find the optimal balance between centralization and decentralization should be considered.

6. The underlying Self-Sovereign Identity network may

be safe, resilient, and decentralized. Nevertheless, the means for establishing trust among the entities and the trust in data, including the verified credentials transmitted, must be meticulously constructed. Data validation may call for a trusted party external to the blockchain network.

7. As a new identification model, Self-Sovereign Identity necessitates a number of system architectural improvements. Important to the success of Self-Sovereign Identity are dependent on the appropriate technology stacks, deployment methods, user experience considerations and operating procedures. Proper design measures must be made to prevent the fate of several other valuable breakthroughs, *e.g.* Pretty Good Privacy [22], which, although being a helpful technology, has not attained the desired level of widespread adoption [23].

8. Self-Sovereign Identity is a relatively new venture with a growing ecosystem, but with limited knowledge on the revenue model [24], and there are user-acceptance concerns [25]. The adoption of new technology by users relies on service providers' support, and vice versa, which might result in the chicken-and-egg dilemma in the Self-Sovereign Identity economic model.

Altogether, there is enough work to be done to lead Self-Sovereign Identity to a successful implementation. In this work the scope will be narrowed to an European Self-Sovereign Identity use case including interoperability of the European Blockchain Services Infrastructure (EBSI) which is a permissioned peer-to-peer network of nodes that operate a blockchain-based services architecture. The next Chapter contains relevant literature and the background necessary to fully comprehend this paper. In Chapter 4, a framework will be devoted to address to the aforementioned issues of Self-Sovereign Identity. Chapter 5 will provide a State-of-the-Art of the eIDAS regulation with regard to the technical implementation of identification and authorization on the highest level of assurance. Furthermore, this Chapter will give an overview and expectation of the coming revised eIDAS regulation, *i.e.* eIDAS2. Furthermore, Chapter 6 will entail the details of the infrastructure necessary to develop a trustworthy Self-Sovereign Identity implementation, consisting of TrustChain, IPv8 and EBSI. Thereafter, Chapter 7 elaborates on the anchors of trust needed to make the Self-Sovereign Identity ecosystem trustworthy. Specifically, these anchors are the Netherlands Chamber of Commerce's Business Register (KVK Handelsregister), Netherlands Vehicle Authory Vehicle Register (RDW kentekenregister) and the Dutch Personal Records Database (BRP). Consecutively, as mentioned as the first challenge in Self-Sovereign Identity, protocols and practices are needed. Accordingly, in Chapter 8 an EBSI implementation at the Dutch Chamber of Commerce and Netherlands Vehicle Authory is realized and discussed. Providing a template for integrating Qualified Trust Service Providers in the EBSI. Lastly, in Chapter 9 a conclusion is drawn and future work is discussed.

# 3 Background

# 4 Design

# 5 eIDAS

# 6 Infrastructure

## 6.1 TrustChain

## 6.2 IPv8

## 6.3 EBSI compliance

# 7 Qualified Trust Service Providers

## 7.1 Legally binded trust

## 7.2 KVK Handelsregister

## 7.3 RDW Vehicle Register

## 7.4 Basisregistratie Personen

# 8 Implementation

# 9 Conclusion

## 9.1 Future Work

- Implement decentralized identification with eIDAS level high assurance.

# References

[1] A. van Huffelen, M. Adriaansens, and D. Yeşilgöz-Zegerius, "Kamerbrief hoofdlijnen beleid voor digitalisering." [Online]. Available: https://www.rijksoverheid.nl/documenten/kamerstukken/2022/03/08/kamerbrief-hoofdlijnen-beleid-voor-digitalisering

[2] Nov 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

[3] Feb 2022. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

[4] U. Leyen, “State of the union address by president von der leyen at the european parliament plenary,” Sep 2020. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

[5] The European Commission, “Article 8(3) of regulation (eu) no 910/2014 of the european parliament and of the council on electronic identification and trust services for electronic transactions in the internal market,” 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1502&from=ES.

[6] V. Mokshagundam, “Top social login tools compared,” Jan 2017. [Online]. Available: https://medium.com/@Vamshi_Mokshagundam/top-social-login-tools-compared-b350eae26118

[7] O. Tene and J. Polonetsky, “Big data for all: Privacy and user control in the age of analytics,” Apr 2013. [Online]. Available: https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1/

[8] eIDAS Expert Group, “The toolbox process,” 2021. [Online]. Available: https://webgate.ec.europa.eu/regdel/web/meetings/2409/documents/6690

[9] D. Mahajan, O. Sperling, and O. White, “Digital id: The opportunities and the risks — mckinsey & company.” [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/digital-id-the-opportunities-and-the-risks

[10] C. Allen, “The path to self-sovereign identity,” Apr 2016. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereregn-identity.html

[11] A. Pfitzmann and M. Hansen, “A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management,” 2010.

[12] T. Speelman, “Self-sovereign identity: Proving power over legal entities,” Jul 2020. [Online]. Available: https://repository.tudelft.nl/islandora/object/uuid%3Aaab1f3ff-da54-47f7-8998-847cb78322c8

[13] Jun 2021. [Online]. Available: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_nl

[14] R. Soltani, U. T. Nguyen, and A. An, “A survey of self-sovereign identity ecosystem,” *Security and Communication Networks*, vol. 2021, pp. 1–26, jul 2021. [Online]. Available: https://doi.org/10.1155%2F2021%2F8873429

[15] H. Montgomery, “Japanese man lost a usb drive with entire city’s personal data after a night out,” Jun 2022. [Online]. Available: https://www.vice.com/en/article/wxn88x/japanese-man-lost-usb-drive-entire-city

[16] M. Brown, “Top 5 biggest lost bitcoin fortunes,” 2022. [Online]. Available: https://www.cryptovantage.com/news/the-top-5-biggest-lost-bitcoin-fortunes-that-we-know-about/

[17] R. Soltani, U. T. Nguyen, and A. An, “Decentralized and privacy-preserving key management model,” in *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, 2020, pp. 1–7.

[18] K. Vidhani, V. Banahatti, and S. Lodha, “Challenges in enabling privacy self management,” *CSI Transactions on ICT*, 10 2021.

[19] Dec 2018. [Online]. Available: https://coinstelegram.com/crypto-alphabet/benefits-and-drawbacks-of-permissioned-blockchains/

[20] M. Sørensen, M. Milkov, and A. K. Angelov, “Decentralized identity management system for self-sovereign identity,” Jun 2018. [Online]. Available: https://projekter.aau.dk/projekter/en/studentthesis/decentralized-identity-management-system-for-selfsovereign-ide
.html

[21] T. Neudecker and H. Hartenstein, “Network layer aspects of permissionless blockchains,” *IEEE Communications Surveys & Tutorials*, vol. PP, pp. 1–1, 09 2018.

[22] S. Garfinkel, D. Russell, and T. Phung, *PGP: Pretty Good Privacy*, ser. Encryption for everyone. O’Reilly Media, Incorporated, 1995. [Online]. Available: https://books.google.nl/books?id=cSe_0OnZqjAC

[23] S. Garfinkel, *Pretty Good Privacy (PGP)*. GBR: John Wiley and Sons Ltd., 2003, p. 1421–1422.

[24] S. Hori, “Self-sovereign identity: future of personal data ownership? — world economic forum,” Aug 2021. [Online]. Available: https://www.weforum.org/agenda/2021/08/self-sovereign-identity-future-personal-data-ownership/

[25] A. Slater, “On self-sovereign identity: What’s the business value of ssi? — hackernoon,” Nov 2019. [Online]. Available: https://hackernoon.com/self-sovereign-identity-what-is-the-business-value-uq6l36wh